



THOMAS L. GARTHWAITE, M.D.
Director and Chief Medical Officer

FRED LEAF
Chief Operating Officer

COUNTY OF LOS ANGELES
DEPARTMENT OF HEALTH SERVICES
313 N. Figueroa, Los Angeles, CA 90012
(213) 240-8101

BOARD OF SUPERVISORS

Gloria Molina
First District

Yvonne Brathwaite Burke
Second District

Zev Yaroslavsky
Third District

Don Knabe
Fourth District

Michael D. Antonovich
Fifth District

March 9, 2005

TO: Each Supervisor

FROM: Thomas L. Garthwaite, M.D.
Director and Chief Medical Officer

SUBJECT: **INFORMATION TECHNOLOGY SUPPORT SERVICES MASTER AGREEMENT (ITSSMA) WORK ORDER EXTENSIONS WITH RYDEK AND 3DI**

This is to notify you of my intent to request the Internal Services Department (ISD) to amend existing ITSSMA Work Order Number N06-0123 with Rydek to extend the term by 17 months and increase the amount by \$212,500 and ITSSMA Work Order Number N06-0126 with 3Di to extend the term by 18 months and increase the Work Order amount by \$225,000 to bring the total for these Work Order extensions to \$437,500. This requested amount with the addition of the existing Work Orders brings the grand total to \$736,500. This request is to extend the services of the consultants to continue implementation and operation of critical network security infrastructure. The extension of the existing Work Orders will exceed the \$300,000 project limit. In accordance with ITSSMA Guidelines, prior Board notice is required for projects that will exceed \$300,000.

BACKGROUND

The current consultants were selected through the ITSSMA competitive bidding process to provide services to the DHS HSA Information Systems Branch (ISB) staff.

Federal, state, and regulatory agency mandates require that DHS implement sufficient security measures on the DHS wide area network (WAN) and local area networks (LAN). As part of the overall design, DHS has implemented a complex security environment utilizing firewalls from several vendors to secure specific segments of the network.

DHS has utilized the ITSSMA process to augment its technical resources and to help the

Department meet its critical Information Technology (IT) needs. By doing so, the Department has been able to draw upon this technical service to improve the efficiency and effectiveness of the Department and meet the various mandates.

Services will be provided to the DHS HSA ISB Technology Services Division (TSD) Infrastructure Security Administration (ISA) Group. The ISA group provides installation, configuration, troubleshooting, maintenance, and technical support for all Firewall, Virtual Private Network (VPN), and Host/Network Intrusion Detection System (HIDS/NIDS) devices. Using these devices, the ISA group secures the DHS network and server resources from Cyber attacks and insures that DHS network communications are HIPAA compliant.

SCOPE OF WORK

The project supported by these ITSSMA contractors is critical to the continued security of the DHS network infrastructure. Under the direction of the County Project Managers, contracted staff will continue to supplement the Department's technical resources on the following areas. The scope of work will remain unchanged:

- **Security Devices Administration.** This includes designing, building, configuring, and managing all firewalls, VPNs, HIDS/ NIDS security devices and supporting the information security infrastructure at all DHS sites.
 - **Firewalls.** Design network topology to support firewall deployment. Create and implement firewall access rules to protect DHS network and resources.
 - **Virtual Private Networks.** Design network topology to support VPN deployment. Create and implement VPNs to secure DHS internal and external network communications.
 - **Implementation.** Implement best practice and HIPAA-compliant procedures for securing firewalls, VPNs, HIDS/NIDS devices and the DHS network. Document all system configurations and security issues.
 - **Monitoring.** Establish centralized management and monitoring systems for all firewall, VPN, HIDS/NIDS devices. Establish and carry out log analysis procedures and security incident respond/reporting procedures.
 - **Maintenance.** Create and institute disaster recovery plans, restoration of service procedures and emergency mode operation procedures.
- **Risk Assessment.** This includes the establishment of procedures for conducting risk assessment, threat analysis and risk management; the identification of security gaps and non-compliance in business processes with respect to HIPAA/security best practices; the development of recommendations for workflow redesign; the assistance with remediation; and training information owners and stakeholders in accurately performing risk assessment/management and threat analysis within their domains.

- **Administration** – This includes other tasks not directly related to the development of information security policies and procedures or training. It includes problem management activities such as tracking, coordination, and management of problem reports and service requests, maintenance of logs and status reports, attending status and other administrative meetings with DHS staff, and any other administrative activities as directed by the DHS Project Manager.
- **Mentoring and Knowledge Transfer** – This includes working with DHS technical staff and facilitating the transition of support responsibilities to DHS technical staff.

JUSTIFICATION

Federal mandates require that DHS develop and implement policies and procedures that (1) safeguard patient protected health information (PHI), (2) prevent and mitigate risks associated with Cyber-Terrorism, and (3) appropriately respond to violations of the DHS information and technology infrastructure. To meet these mandates, highly skilled technical staff is needed to support the design, setup and configuration, implementation, monitoring, maintenance and support of various security devices including firewalls, firewall rule sets, VPNs, VPN policies, HIDS, or NIDS.

County staff is not available to provide these essential functions. DHS has aggressively sought to hire County personnel to fill vacant technology positions; however, our best efforts have been unsuccessful. While we have filled some vacant positions, we still are challenged to recruit qualified staff. Consequently, we utilize ITSSMA to supplement our existing IT security staff. The consultants perform highly specialized and technical functions, and have extensive knowledge of DHS systems. They have acquired detailed knowledge of our technical infrastructure and network topologies. In addition, they are experienced with the Department's computer-related equipment installations, software, system applications, and network configuration and have an understanding of our business process and procedures. Continued use of the consultants will allow the Department to maintain the level of IT expertise needed, and currently unavailable within the Department.

While the Department recognizes that reliance on contract consultants may not be ideal, we continue to be unable to attract comparably qualified permanent replacements within the allocation of items available to us. Although several exams have been administered, the results have not produced candidates with the skills and experience required to perform these technically specialized functions. These experienced consultants will facilitate knowledge transfer and mentoring of DHS staff and the eventual transition of support to County employees.

The services received under the ITSSMA Work Orders are essential to the effective security infrastructure of our department. Therefore, it is necessary to retain experienced consultants who have gained first-hand knowledge of our operations and business systems, to ensure that DHS is HIPAA compliant and that the DHS network and systems infrastructure is secured from cyber attacks.

FISCAL IMPACT

The contractor rates remain the same for the Work Orders that are being extended. The maximum County obligation under these two Work Orders including the extensions is as follows:

Work Order NO6-0123	
Current Maximum Amount (Term of 2/23/04 – 4/01/05)	\$140,500
Extension (4/02/05 – 9/01/06)	\$212,500
Subtotal	<u>\$353,000</u>

Work Order N06-0126	
Current Maximum Amount (Term of 2/17/04 – 3/25/05)	\$158,500
Extension (3/26/05 – 9/25/06)	\$225,000
Subtotal	<u>\$383,500</u>

Grand Total for both Work Orders	<u>\$736,500</u>
----------------------------------	------------------

CLOSING

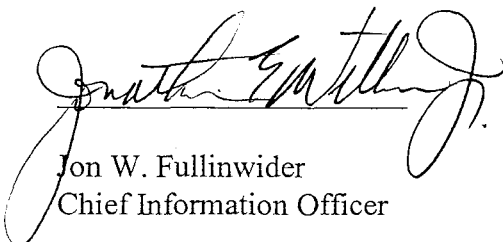
Consistent with ITSSMA policies and procedures, we are informing your Board of our intention to extend the term of these Work Orders and increase the maximum amount of each. In two weeks time we will instruct ISD to proceed with the amendments.

If you have any questions or require additional information, please let me know.

TLG:gc

c: Executive Officer, Board of Supervisors
Chief Administrative Officer
Chief Information Officer
County Counsel
Director, Internal Services Department

NOTED AND APPROVED:


Jon W. Fullinwider
Chief Information Officer

Received by CIO: 03-18-2005
